International Law Studies - Volume 76
Computer Network Attack and International Law
Michael N. Schmitt & Brian T. O'Donnell (Editors)

XI

Wired Warfare: Computer Network Attack and the *Jus in Bello*

Michael N. Schmitt

Despite ongoing debates about the existence, or lack thereof, of a "revolution in military affairs," it is undeniable that 21st century warfare will differ dramatically from that which characterized the 20th. Perhaps most remarkable will be the maturation of "information warfare" as a tool of combat.[1] It will challenge existing warfighting doctrine, necessitate a reconceptualization of the battlespace, and expand the available methods and means of warfare. Of particular note will be the impact of information warfare on the principles of international humanitarian law . . . and vice versa.

Information warfare (IW), in particular computer network attack, has been described in detail in this volume and elsewhere. Therefore, only a brief explanation of the typology employed in this chapter is necessary. Information warfare is a subset of information operations (IO), i.e., "actions taken to affect adversary information and information systems while defending one's own information and information systems."[2] Such operations encompass virtually any nonconsensual measures intended to discover, alter, destroy, disrupt, or transfer data stored in a computer, manipulated by a computer, or transmitted through a computer. They can occur in peacetime, during crises, or at the strategic, operational, or tactical levels of armed conflict.[3] Information operations are distinguished by that which is affected or protected—information.

IW is narrower. It consists of "information operations conducted during time of crisis or conflict to achieve or promote specific objectives over a specific adversary or adversaries."[4] Thus, information warfare is differentiated from other operations by the context in which it occurs—crisis or conflict. As an example, routine peacetime espionage is an example of an information operation that does not constitute information warfare unless conducted during a crisis or hostilities.

Computer network attacks (CNA), which may amount to IW or merely IO, are "operations to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves."[5] The essence of CNA is that, regardless of the context in which it occurs, a data stream is relied on to execute the attack.[6] Thus, the *means* used set CNA apart from other forms of IO. These means vary widely. They include, *inter alia,* gaining access to a computer system so as to acquire control over it, transmitting viruses to destroy or alter data, using logic bombs that sit idle in a system until triggered on the occasion of a particular occurrence or at a set time, inserting worms that reproduce themselves upon entry to a system thereby overloading the network, and employing sniffers to monitor and/or seize data.

This chapter addresses the use of CNA during *international* armed conflict and is limited to consideration of the *jus in bello,* that body of law addressing what conduct is permissible, or impermissible, during hostilities, irrespective of the legality of the initial resort to force by the belligerents.[7] Discussion therefore centers on the use of CNA in the context of "State-on-State" armed conflict. Moreover, the chapter is an effort to explore the *lex lata,* rather than an exercise in considering *lex ferenda.* While setting forth *lex ferenda* is an especially worthy project as the nature of warfare evolves,[8] the goal here is simply to analyze the applicability of existing humanitarian law to computer network attack, and identify any prescriptive lacunae that may exist therein.

Applicability of Humanitarian Law to CNA

The threshold question is whether computer network attack is even subject to humanitarian law. To begin with, there is no provision in any humanitarian law instrument that directly addresses CNA, or, for that matter, IW or IO; this might suggest that CNA is as yet unregulated during armed conflict. Additionally, it could be argued that the development and employment of CNA post-dates existing treaty law, and thus, having not been within the contemplation of the Parties to those instruments, is exempt from the coverage thereof. A third possible argument for inapplicability is that humanitarian law

is designed for methods and means that are kinetic in nature; since there is little that is "physical" in CNA, attacks by computers fall outside the scope of humanitarian law.[9] Restated, humanitarian law applies to armed conflict, and computer network attack is not "armed."

The first two possibilities are easily dispensed with. The fact that existing conventions are silent on CNA is of little significance. First, the Martens clause, a well-accepted principle of humanitarian law, provides that whenever a situation is not covered by an international agreement, "civilians and combatants remain under the protection and authority of the principles of international law derived from established custom, from the principles of humanity and from the dictates of public conscience."[10] By this norm, all occurrences during armed conflict are subject to application of humanitarian law principles; there is no lawless void. The acceptance of "international custom" as a source of law in Article 38 of the Statute of the International Court of Justice also demonstrates the fallacy of any contention of inapplicability based on the absence of specific *lex scripta*.[11]

Arguments focusing on the fact that CNA post-dates present prescriptive instruments are similarly fallacious. Precisely this line of reasoning was presented to the International Court of Justice in *Legality of the Threat or Use of Nuclear Weapons*. In its advisory opinion, the court summarily rejected the assertion that because humanitarian "principles and rules had evolved prior to the invention of nuclear weapons," humanitarian law was inapplicable to them. As the court noted, "[i]n the view of the vast majority of States as well as writers there can be no doubt as to the applicability of humanitarian law to nuclear weapons."[12] There being no reason to distinguish nuclear from computer weapons, at least on the basis of when they were developed vis-à-vis the entry into force of relevant humanitarian law norms, the same conclusion applies to CNA. Furthermore, a review of new weapons and weapon systems for compliance with humanitarian law is a legal, and often a policy, requirement.[13] Obviously, this would not be so if pre-existing law were inapplicable, *ab initio*, to nascent methods and means of warfare.

This analysis leaves only the third argument for inapplicability of humanitarian law to computer network attack—that it is not *armed* conflict, at least not in the absence of conventional hostilities. In exploring this prospect one might reflexively reach, as some have, for the UN Charter.[14] Article 2(4) of that constitutive instrument proscribes the "use of force," whereas Article 51 allows for forceful action in self-defense in the face of an "armed attack." If an act constitutes a "use of force" or an "armed attack" would it not logically be subject to the laws of "armed conflict," i.e., humanitarian law? If so, all that need be done is to determine what actions amount to a use of force or constitute an armed attack.[15]

Such an analysis confuses the *jus ad bellum* with the *jus in bello*. Articles 2(4) and 51, together with Chapter VII of the Charter, are the key prescriptive norms of the *jus ad bellum*. They govern when it is legitimate under international law (or at least Charter law) to resort to force, either as a tool of national policy or in the face of another State's decision to do so in pursuit of its own national interests. A State that has unlawfully resorted to force may subsequently carry out its operations in compliance with the *jus in bello*, which, as mentioned *supra*, governs the actual conduct of hostilities by the parties. For instance, during the Falklands/Malvinas conflict Argentina wrongfully invaded British territory, but generally abided by the rules of warfare. Similarly, many commentators urge that Operation ALLIED FORCE, NATO's 1999 Kosovo bombing campaign, violated the *jus ad bellum*, but was conducted in substantial compliance with the laws governing armed conflict.[16] Conversely, a State (or its military) that lawfully resorts to force may subsequently violate humanitarian law principles. As an example, it seems clear that Russia is entitled to maintain order in Chechnya; but it is equally clear that in doing so its forces have regularly violated both the law of non-international armed conflict and human rights law.[17] The point is that the *jus ad bellum* and *jus in bello* are normatively distinct. Professor Leslie Green has very pragmatically noted this distinction and its relevance to military personnel:

> Members of the armed forces are not concerned with the manner in which a conflict begins, nor whether it is legal or illegal. So far as they are concerned, the law of armed conflict comes into operation and they must abide by it from the moment that hostilities begin and they are required to participate therein.[18]

The task at hand, therefore, is to query when "hostilities" have begun. Tautologically, the answer is that hostilities commence once humanitarian law applies. Common Article 2 to the four 1949 Geneva Conventions provides that the conventions apply, aside from specific provisions that pertain in peacetime, "to all cases of declared war or of any other *armed conflict* which may arise between two or more of the High Contracting Parties, even if the state of war is not recognized by one of them."[19] The 1977 Protocol Additional I, which, like the conventions pertains to international armed conflict, adopts the same "armed conflict" standard, one that has become an accepted customary law threshold for humanitarian law.[20] The fact that the 1977 Protocol Additional II also embraces the term "armed conflict,"[21] albeit in the context of *non*-international armed conflict, demonstrates that armed conflict is a condition determined by its nature, rather than its participants,[22] location,[23] or, as was formerly the case with "war," declaration of the belligerents.[24]

It seems relatively clear, then, that humanitarian law is activated through the commencement of armed conflict. But what is armed conflict? Commentaries published by the International Committee of the Red Cross to the 1949 Geneva Conventions and the 1977 Protocols Additional take a very expansive approach towards the meaning of the term. The former define armed conflict as "[a]ny difference arising between two States and leading to the *intervention of armed forces* . . . even if one of the Parties denies the existence of a state of war. It makes no difference how long the conflict lasts, or how much slaughter takes place."[25] Similarly, Protocol Additional I's commentary provides that "humanitarian law . . . covers any dispute between two States involving the *use of their armed forces*. Neither the duration of the conflict, nor its intensity, play a role. . . ."[26] Protocol Additional II's commentary describes armed conflict as "the existence of open *hostilities between armed forces* which are organized to a greater or lesser degree."[27] The *sine qua non* in all three cases is commitment of armed forces.

But a dispute or difference resulting in the engagement of armed forces cannot be the sole criterion. Military forces are used on a regular basis against adversaries without necessarily producing a state of armed conflict—consider aerial reconnaissance/surveillance operations as just one example. Further, it is now generally accepted that isolated incidents such as border clashes or small-scale raids do not rise to the level of armed conflict as that term is employed in humanitarian law.[28] Accordingly, State practice, supplemented by the writings of publicists, illustrates that Protocol Additional I's dismissal of intensity and duration has proven slightly overstated.

Instead, the reference to armed forces is more logically understood as a form of prescriptive shorthand for activity of a particular nature and intensity. At the time the relevant instruments were drafted, *armed* forces were the entities that conducted the contemplated activity at the requisite level of intensity; by focusing on the armed forces, the intended ends were achieved. Restated, the relevant provisions of the conventions and their commentaries were actor-based because citing the actors engaged in the undesirable conduct—armed forces—was, at the time, a convenient and reliable method for regulating it.

And what was that conduct? The logical answer is found in the underlying purposes of humanitarian law. A review of its instruments and principles makes clear that protecting individuals who are not involved in the hostilities directly, as well as their property, lies at their core.[29] Most notably, protected entities include civilians and civilian objects, as well as those who are *hors de combat* (e.g., wounded or captured personnel) or provide humanitarian services (e.g., medical personnel). As for the protection they are entitled to, it is usually framed in terms of injury or death or, in the case of property, damage or

destruction. These Geneva law purposes are complemented by Hague law norms intended to limit suffering generally through restrictions on certain weaponry and methods of warfare.[30]

This excessively abbreviated summarization of humanitarian law's fundamental purposes elucidates the term armed conflict. Armed conflict occurs when a group takes measures that injure, kill, damage, or destroy. Also included are actions intended to cause such results or in which they are the foreseeable consequences thereof. Because the issue is the *jus in bello* rather than *ad bellum*, the motivation underlying the actions is irrelevant. So too is their wrongfulness or legitimacy. Thus, for example, the party that commences the armed conflict by committing such acts may be acting in legitimate anticipatory (or interceptive) self-defense; nevertheless, as long as the actions were intended to injure, kill, damage, or destroy, humanitarian law governs them. It should be noted that given the current weight of opinion, actions that are sporadic or isolated in nature would not suffice. Additionally, because the issue is the law applicable to international armed conflict, the relevant actions must be attributable to a State.[31]

Returning to the topic at hand, and quite aside from *ad bellum* issues, humanitarian law principles apply whenever computer network attacks can be ascribed to a State, are more than merely sporadic and isolated incidents, and are either intended to cause injury, death, damage, or destruction (and analogous effects), or such consequences are foreseeable. This is so even though classic *armed* force is not being employed. By this standard, a computer network attack on a large airport's air traffic control system by agents of another State would implicate humanitarian law. So too would an attack intended to destroy oil pipelines by surging oil through them after taking control of computers governing flow,[32] causing the meltdown of a nuclear reactor by manipulation of its computerized nerve center, or using computers to trigger a release of toxic chemicals from production and storage facilities. On the other hand, humanitarian law would not pertain to disrupting a university intranet, downloading financial records, shutting down Internet access temporarily, or conducting cyber espionage because, even if part of a regular campaign of similar acts, if the foreseeable consequences would not include injury, death, damage, or destruction.

It should be apparent that, given advances in methods and means of warfare, especially information warfare, it is no longer sufficient to apply an actor-based threshold for application of humanitarian law; instead, a consequence-based one is more appropriate. This is hardly a jurisprudential epiphany. No one would deny, for instance, that biological or chemical warfare (which does not involve delivery by kinetic weapons) is subject to humanitarian law. A

consequence-based threshold is also supported by the fact that once armed conflict has commenced (and except for prohibitions relevant to particular weapons), the means by which injury, death, damage or destruction are produced have no bearing on the legality of the causal act. Intentionally targeting a civilian or other protected persons or objects is unlawful irrespective of the method or means used. Starvation, suffocation, beating, shooting, bombing, even cyber attack—all are subject to humanitarian law based on the fact that a particular consequence results. That this is so counters any assertion that, standing alone, cyber attacks are not subject to humanitarian law because they are not "armed" force. On the contrary, they may or may not be, depending on their nature and likely consequences.

Computer Network Attack Targets

As has been discussed, computer network attacks are subject to humanitarian law if they are part and parcel of either a classic conflict or a "cyber war" in which injury, death, damage, or destruction are intended or foreseeable. This being so, it is necessary to consider the targets against which computer network attacks may be directed.

A useful starting point is to frame the conduct that is subject to the prescriptive norms governing targeting. Because most relevant Protocol Additional I provisions articulate standards applicable to Parties and non-Parties (as a restatement of binding customary law) alike, that instrument serves as an apt point of departure.[33] Article 48, the basic rule governing the protection of the civilian population, provides that "Parties to the conflict . . . shall direct their operations only against military objectives."[34] On its face, Article 48 would seem to rule out *any* military operation, including CNA, directed against other than purely military objectives. In fact, it does not. In subsequent articles, proscriptions are routinely expressed in terms of "attacks." Thus, "the civilian population as such, as well as individual civilians, shall not be the object of attack"[35]; "civilian objects shall not be the object of attack"[36]; "indiscriminate attacks are forbidden"[37]; "attacks shall be limited strictly to military objectives"[38]; and so forth. The term is expressly defined in Article 49: "'Attacks' means acts of violence against the adversary, whether in offence or in defence." As a general matter then, the prohibition is not so much on targeting non-military objectives as it is on *attacking* them, specifically through the use of violence. This interpretation is supported by the text of Article 51, which sets forth the general principle that the "civilian population and individual civilians shall enjoy general protection against *dangers* arising from military operations," and which prohibits "acts or threats of *violence*

the primary purpose of which is to spread terror among the civilian population,"[39] as well as the commentary to Article 48, which notes that "the word 'operation' should be understood in the context of the whole of the Section; it refers to military operations during which *violence* is used."[40]

In light of this interpretation, does computer network attack fall outside the ambit of "attacks" because it does not employ violence? No, and for precisely the same reason that armed attacks can include cyber attacks. "Attacks" is a term of prescriptive shorthand intended to address specific consequences. It is clear that what the relevant provisions hope to accomplish is shielding protected individuals from injury or death and protected objects from damage or destruction. To the extent the term "violence" is explicative, it must be considered in the sense of violent *consequences* rather than violent *acts*. Significant human physical or mental suffering[41] is logically included in the concept of injury; permanent loss of assets, for instance money, stock, etc., directly transferable into tangible property likewise comprises damage or destruction. The point is that inconvenience, harassment, or mere diminishment in quality of life does not suffice; human suffering is the requisite criterion. As an example, a major disruption of the stock market or banking system might effectively collapse the economy and result in widespread unemployment, hunger, mental anguish, etc., a reality tragically demonstrated during the Depression of the 1930s. If it did cause this level of suffering, the CNA would constitute an attack, as that term is understood in humanitarian law.

Other articles within the section sustain this reading. For instance, the rules of proportionality speak of "loss of civilian life, injury to civilians, damage to civilians objects, or a combination thereof,"[42] those relating to protection of the environment refer to "widespread, long-term, and severe damage,"[43] and the protection of dams, dykes, and nuclear electrical generating stations is framed in terms of "severe losses among the civilian population."[44] Furthermore, during the negotiation of Protocol Additional I, the issue of whether laying landmines constituted an attack arose. Most agreed that it did because "there is an attack whenever a person is directly endangered by a mine laid."[45] By analogy, a computer network attack which foreseeably endangers protected persons or property would amount to an attack.

Return now to Article 48. In the context of computer network attack, and as a general rule (various other specific prohibitions are discussed *infra*), the article would prohibit those CNA operations directed against non-military objectives that are intended to, or would foreseeably, cause injury, death, damage, or destruction. Unless otherwise prohibited by specific provisions of humanitarian law, CNA operations unlikely to result in the aforementioned consequences are

permissible against non-military objectives, such as the population.[46] As a result of this distinction, the need to carefully assess whether or not an information warfare operation is or is not an "attack" is greatly heightened. In the past, analysis of this matter approximated a *res ipsa loquitor* approach. However, CNA is much more ambiguous than traditional military operations, thereby demanding a more challenging consequence-based consideration.

While CNA does dramatically expand the possibilities for "targeting" (but not attacking) non-military objectives, it is unfair to characterize this as a weakening of the prescriptive architecture. Instead, it simply represents an expansion of permissible methods and means resulting from advances in technology; existing norms remain intact. Recall, for example, that psychological operations directed against the civilian population that cause no physical harm are entirely permissible, so long as they are not intended to terrorize.[47] This is so whether the motivation for the operations is military in nature or not. Nevertheless, although the objective regime is a constant, the advent of CNA reveals a normative lacuna that, unless filled, will inevitably result in an expansion of war's impact on the civilian population.

Assuming a CNA operation is an "attack," what can be targeted? Analytically, potential targets can be classified into three broad categories: 1) combatants and military objectives; 2) civilians and civilian objects; and 3) dual-use objects. Moreover, particular types of potential targets enjoy specific protection. It is useful to address each grouping separately.

Combatants and military objectives: Combatants and military objectives are by nature valid targets and may be directly attacked as long as the method used, as discussed in the next section, is consistent with humanitarian law restrictions. Those who plan or decide on attacks have an affirmative duty to "do everything feasible" to verify that intended targets are legitimate, i.e., that they do not enjoy immunity from attack under humanitarian law.[48]

A combatant is a member of the armed forces other than medical personnel and chaplains; armed forces include "all organized armed forces, groups and units which are under a command responsible to [a Party to the conflict] for the conduct of its subordinates. . . . [They must] be subject to an internal disciplinary system which, *inter alia*, shall enforce compliance with the rules of international law applicable in armed conflict."[49] Directing computer network attacks against combatants, for instance by causing a military air traffic control system to transmit false navigational information in order to cause a military troop transport to crash, is clearly permissible.

Military objectives are defined in Article 52 of Protocol Additional I as "those objects which by their nature, location, purpose or use make an effective

contribution to military action and whose total or partial destruction, capture or neutralization, in the circumstances ruling at the time, offers a definite advantage."[50] Military equipment and facilities, other than medical and religious items, are clearly military objectives, and thereby subject to direct computer network attack. However, determining which objects are military objectives beyond these obvious exemplars is often difficult.[51] The problem lies in ascertaining the required nexus between the object to be attacked and military operations.

The crux of the dilemma is interpretation of the terms "effective" and "definite." Some, such as the International Committee of the Red Cross, define them very narrowly. In the ICRC commentary to the protocol, effective contribution includes objects "directly used by the armed forces" (e.g., weapons and equipment), locations of "special importance for military operations" (e.g., bridges), and objects intended for use or being used for military purposes.[52] As to "definite military advantage," the commentary excludes attacks that offer only a "potential or indeterminate" advantage.[53] By contrast, the United States, which does not dispute the wording of the definition, would include economic targets that "indirectly but effectively support and sustain the enemy's war-fighting capability," a particularly expansive interpretation.[54]

This difference has interesting implications for computer network attack. Can a banking system be attacked because wealth underpins a military's sustainability? What about the ministry responsible for taxation? The stock market? Are attacks on brokerage firms acceptable because they will undermine willingness to invest in the economy? If a country disproportionately relies on a particular industry to provide export income (e.g., oil), can computer network attack be used to disrupt production and distribution? The issue of striking economic targets is a particularly acute one because the operation of most is computer intense in nature, and thereby very appealing to information warfare targeteers.

The threshold issue, recalling the discussion *supra*, is whether or not the attack would cause injury, death, damage, or destruction. Once this determination is made, the differing interpretations of military objective would come into play, in all likelihood leading to disparate results on the legitimacy of striking the target. On the other hand, if the operation were designed to cause, e.g., mere inconvenience, it would not rise to the level of an attack and would thus be permissible regardless of the target's nexus, or lack thereof, to military operations. For instance, if the Serbian State television station had been targeted by CNA rather than kinetic weapons during NATO strikes on Belgrade in April 1999, there might well have been no consequent injury, death, damage, or destruction; in that circumstance, criticism on the basis that a civilian target had

been hit would likely have fallen on deaf ears, thereby probably avoiding the negative publicity that resulted, as well as the pending litigation in the European Court of Human Rights.[55]

Civilians and civilian objects: Civilians are those not considered combatants,[56] whereas a civilian object is one that is not a military objective.[57] The prohibition on attacking civilians and civilian objects is nearly absolute. Specifically, Protocol Additional I provides:

> Article 51.2. The civilian population, as such, as well as individual civilians shall not be the object of attack. Acts or threats of violence the primary purpose of which is to spread terror among the civilian population are prohibited.
>
> Article 52. Civilian objects shall not be the object of attack or of reprisals.[58]

Doubts as to the character of an object or individual are to be resolved in favor of finding civilian status.[59] Again, in the case of computer network attack, the threshold question is whether or not the attack is intended to, or forseeably will, cause injury, death, damage, or destruction; if so, the prohibitions set forth earlier, which undeniably restate existing customary law, apply.

Unfortunately, the norms, albeit clear on their face, are subject to interpretive difficulties. The differing standards for distinguishing civilian objects from military objectives have already been highlighted. Similar disparities surround when a civilian may be attacked. Protocol Additional I allows for this possibility only in the case of a civilian taking a "direct part in hostilities," a standard described in the commentary as "acts of war which by their nature or purpose are likely to cause actual harm to the personnel or equipment of the enemy armed forces."[60] This is the illegal combatant problem. Some would limit civilian immunity even more severely by, for instance, characterizing mission-essential civilians working at a base during hostilities, though not engaged directly in acts of war, as legitimate targets.[61]

In the context of information operations, the civilian issue is an important one. Some countries have elected to contract out information warfare functions, whether those functions involve the maintenance of assets or the conduct of operations. Moreover, computer network attack is a function that may be tasked to government agencies other than the military. In the event civilian contractors or non-military personnel are in a support role that is essential to the conduct of operations, for instance maintaining CNA equipment, by the latter interpretation they would be directly targetable. Further, because they are valid targets, any injury caused them would not be calculated when assessing whether

an attack is proportional (see discussion *infra*). On the other hand, narrowly applying the "direct part in hostilities" standard would preserve the protection they enjoy as civilians, though if captured they would be entitled to prisoner of war status as persons "accompanying the armed forces."[62]

Should civilians engage in computer network attack themselves, the problem becomes more complex. If the CNA results, or foreseeably could result, in injury, death, damage, or destruction, then the "perpetrators" would be illegal combatants. This status attaches because they have taken a direct part in hostilities without complying with the criteria for characterization as a combatant. As illegal combatants, they may be directly attacked, any injury suffered by them would be irrelevant in a proportionality calculation, and in the event of their capture they would not be entitled to prisoner of war status.

By contrast, if the civilians involved were conducting computer network operations that did not rise to the level of "attacks," they would not be illegal combatants because they would have committed no "acts of war that by their nature or purpose are likely to cause actual harm to the personnel or equipment of the enemy armed forces." Their civilian status and its corresponding protections would remain intact. Nevertheless, as with support personnel, if captured while attached to a military unit and accompanying that unit, these civilians would be classed as prisoners of war.[63] Of course, the facility and equipment being used to conduct the operations might well be valid military objectives and, as a result, be subject to attack; but the operators themselves could not be directly attacked.

As should be apparent, the use of civilians, whether contractors or government employees, is fraught with legal pitfalls. Clearly, a prudent approach would be to employ military personnel for information warfare purposes.

Dual-use objects: A dual-use object is one that serves both civilian and military purposes. Examples of common dual-use objects (or objectives) include airports, rail lines, electrical systems, communications systems, factories that produce items for both the military and the civilian population, and satellites such as INTELSAT, EUROSAT and ARABSAT. If an object is being used for military purposes, it is a military objective vulnerable to attack, including computer network attack. This is true even if the military purposes are secondary to the civilian ones.

Several caveats are in order. First, whether or not an object is a military objective may turn on whether the narrow or broad definition of the term, a matter discussed *supra*, is used. Second, whether an object is dual-use, and therefore a military objective, will depend on the nature of the specific conflict. An airfield may be utilized for logistics purposes in one conflict, but serve no military function in another. Third, an object that has the potential for military usage, but is

presently solely used for civilian purposes, is a military objective if the likelihood of use is reasonable and not remote in the context of the particular conflict underway. Finally, dual-use objects must be carefully measured against the requirements of discrimination and proportionality, discussed *infra,* because by definition an attack thereon risks collateral damage and incidental injury to civilians or civilian objects.

Specifically protected objects: In addition to the general rules regarding the protection of the civilian population, certain objects enjoy specific protection. A controversial category of specially protected objects is dams, dikes, and nuclear electrical generating stations. Because of their reliance on computer and computer networks, such facilities are especially vulnerable to CNA. Article 56 of Protocol Additional I, a provision opposed by the United States, forbids an attack on these facilities if the attack might "cause the release of dangerous forces [e.g., water or radioactivity] and consequent severe losses among the civilian population."[64] This prohibition applies even if they are military objectives. Interestingly, CNA offers a fairly reliable means of neutralizing such facilities without risking the release of dangerous forces, a difficult task when using kinetic weapons.

Conducting attacks that starve the civilian population or otherwise deny it "indispensable objects,"[65] even if enemy armed forces are the intended "victims," is prohibited.[66] Indispensable objects include such items as foodstuffs, crops, livestock, or drinking water. Applying this restriction, computer networks attacks against, for instance, a food storage and distribution system or a water treatment plant serving the civilian population would be impermissible even if military forces also rely on them.

Protocol Additional I further prohibits military operations likely to cause widespread, long-term, and severe damage to the environment,[67] although the United States does not recognize the provision as a restatement of customary law. Computer network attacks might conceivably cause such devastation. An attack on a nuclear reactor could result in a meltdown of its core and consequent release of radioactivity. Similarly, CNA could be used to release chemicals from a storage or production facility or rupture a major oil pipeline. Many other possibilities for the causation of environmental damage through CNA exist. It is important to note that the prohibition applies regardless of whether or not the attack is targeted against a valid military objective and even if it complies with the principle of proportionality. Once the requisite quantum of damage is expected to occur, the operation is prohibited.

There are a number of other objects, persons, and activities that enjoy special protected status, and which are susceptible to computer network attack, but which do not present unique CNA opportunities or challenges. For example,

military and civilian medical units and supplies are exempt from attack unless being used for military purposes;[68] the same is generally true of medical transport.[69] So too are cultural objects, places of worship,[70] and civil defense shelters, facilities, and material.[71] Additionally, humanitarian relief activities must not be interfered with.[72] By these prohibitions, for example, a computer network attack to alter blood type information in a hospital's data bank, deny power to a bomb shelter, or misroute humanitarian relief supplies would all be unlawful. Of course, misuse of protected items or locations for military purposes renders them valid military objectives that may be attacked.

Finally, there are limitations on striking certain objects or individuals in reprisal, including reprisals by computer network attack. Reprisals are otherwise unlawful actions taken during armed conflict in response to an adversary's own unlawful conduct. They must be designed solely to cause the adversary to act lawfully, be preceded by a warning (if feasible), be proportionate to the adversary's violation, and cease as soon as the other side complies with the legal limitations on its conduct. The right to conduct reprisals has been severely restricted in treaty law, much of which expresses customary law. There are specific prohibitions on reprisals conducted against civilians; prisoners of war; the wounded, sick, and shipwrecked; medical and religious personnel and their equipment; protected buildings, equipment, and vessels; civilian objects; cultural objects; objects indispensable for the survival of the civilian population; works containing dangerous forces; and the environment.[73] Essentially, this leaves only combatants and military objectives subject to reprisals. Of course, in most cases a computer network attack conducted against them would be lawful at any rate.[74]

In fairness, it should be acknowledged that certain countries argue that the Protocol Additional I restrictions on reprisals fail to reflect customary law. The United States, while accepting that most reprisals against civilians would be inappropriate (and illegitimate), asserts that the absolute prohibition thereon "removes a significant deterrent that presently protects civilians and other war victims on all sides of the conflict."[75] The United Kingdom issued a reservation on precisely the same point when it became a Party to the protocol.[76] For these and other countries that have adopted this position, reprisatory computer network attacks are issues of policy, not law.

Limits on Striking Legitimate Targets

The core prescriptions on striking legitimate targets are based in the principle of discrimination.[77] It is this principle which most clearly expresses humanitarian law's balancing of State-centric interests in resorting to force against the

more broadly based humanitarian interest in shielding non-participants from the effects of what is, at best, an unfortunate necessity.

Discrimination is bifurcated in nature. Applied to weapons, it limits the use of those that are incapable of distinguishing between combatants and military objectives on the one hand and civilians, civilian objects, and other protected entities on the other. Applied to tactics and the *use* of weapons, it requires an effort to distinguish between the two categories when conducting military operations. Protocol Additional I articulates this difference in Article 51.4:

> Indiscriminate attacks are: (a) those which are not directed at a specific military objective; (b) those which employ a method or means of combat which cannot be directed at a specific military objective; or (c) those which employ a method or means of combat the effects of which cannot be limited as required by this Protocol; and consequently, in each such case, are of a nature to strike military objectives and civilians or civilian objects without distinction.

Subparagraph (a) refers to indiscriminate use, whereas (b) and (c) describe indiscriminate weapons. The indiscriminate use aspect of discrimination consists of three related components—distinction, proportionality, and minimizing collateral damage and incidental injury.[78]

Indiscriminate weapons: Computer network attacks are mounted by a weapon system consisting of a computer, computer code, and a means by which that code is transmitted. Obviously, the computer itself is not indiscriminate for it can very discretely send code to particular computers and networks. The sending of e-mail is an apt example. By contrast, code can be written that is very, perhaps intentionally, indiscriminate. The classic example is a virus that passes from computer to computer free from the control of its originator. Because the code, even if an uncontrollable virus, can be targeted at particular military objectives, it is not indiscriminate on the basis that it cannot be directed. However, such code may be indiscriminate on the ground that its *effects* cannot be limited. In many cases, once viral code is launched against a target computer or network, the attacker will have no way to limit its subsequent retransmission. This may be true even in a closed network, for the virus could, as an example, be transferred into it by diskette. Simply put, malicious code likely to be uncontrollably spread throughout civilian systems is prohibited as an indiscriminate weapon.

One must be careful not to overstate the restriction. Note that Article 51.4 cites "methods and means of combat." A means of combat is defined in Protocol Additional I's commentary as a "weapon," whereas a method of combat is the way a weapon is used.[79] The plain meaning of "weapon" is something that

can be used to *attack* an adversary. Drawing on the analysis *supra* regarding the humanitarian law term "attacks," computer code is only part of a *weapon* system when it can cause the effects encompassed in that term—injury, death, damage, and destruction (including related effects like severe mental suffering, terror, suffering, etc.). In the event it cannot, it is not part of a weapon system, and thus would not be prohibited, at least not on the ground that it is indiscriminate.

Distinction: The principle of distinction, unquestionably part of customary humanitarian law, is set forth in Protocol Additional I, Article 48: "[T]he Parties to the conflict shall at all times distinguish between the civilian population and combatants and between civilian objects and military objectives and accordingly shall direct their operations only against military objectives." Whereas the prohibition on attacking civilians directly rendered a specific category of potential targets off-limits, the distinction requirement extends protection to cases in which an attack may not be directed against civilian or civilian objectives specifically, but in which there is a high likelihood of striking them nonetheless. An example would be firing a weapon, though capable of being aimed, blindly.

This is a particularly relevant prohibition in the context of computer network attack. For example, it would embrace situations where it is possible to discretely target a military objective through a particular means of CNA, but instead a broad attack likely to affect civilian systems is launched. Such an attack would be analogous to the Iraqi SCUD attacks against Saudi and Israeli population centers during the 1990–91 Persian Gulf War.[80] The SCUD is not an inherently indiscriminate weapon. Indeed, it is easily capable of being aimed with sufficient accuracy against, for instance, military formations in the desert. However, use of SCUDS against population centers was indiscriminate even if the Iraqi intent was to strike military objectives situated therein; the likelihood of striking protected persons and objects so outweighed that of hitting legitimate targets that the use was improper. Given the interconnectivity of computer systems today, computer network attacks could readily be launched in an analogous fashion.

Proportionality: Scienter distinguishes the principle of proportionality from that of distinction. Distinction limits direct attacks on protected persons or objects and those in which there is culpable disregard for civilian consequences. By contrast, proportionality governs those situations in which harm to protected persons or objects is the foreseeable consequence of an attack, but not its intended purpose. The principle is most often violated (sometimes in an unintended but culpably negligent fashion) as a result of: 1) lack of sufficient knowledge or understanding of what is being attacked; 2) an inability to surgically craft the

amount of "force" being applied against a target; and 3) the inability to ensure the weapon strikes precisely the right aim point.[81] All three pitfalls could surface in the context of computer network attack.

As set forth in Protocol Additional I, an attack is indiscriminate as violative of the principle of proportionality when it "may be expected to cause incidental loss of civilian life, injury to civilians, damage to civilian objects, or a combination thereof, which would be excessive in relation to the concrete and direct military advantage anticipated."[82] A concrete and direct advantage is "substantial and relatively close[;] . . . advantages which are hardly perceptible and those which would only appear in the long term should be disregarded."[83] Moreover, the advantage calculated is that resulting from the overall operation, not the individual attack itself.[84]

Basically, the principle of proportionality mandates a balancing test—one that is especially difficult to conduct because differing entities (suffering and damage v. military advantage) are being compared against each other in the absence of a common system of valuation. How should civilian passenger lives be weighed against military aircraft in a computer network attack on an air traffic control system? How much human suffering is acceptable when shutting down an electrical grid that serves both military and civilian purposes? Can computer network attacks be conducted against telecommunications if they result in degrading emergency response services for the civilian population? Complicating matters is the fact that the answers to these and similar questions, assuming there are any "right" answers, is contextual because the military advantage resulting from an attack always depends on the state of hostilities at the time.[85] Acknowledging the difficulty involved in making these types of determinations, the Protocol Additional I commentary notes that "[p]utting these provisions into practice . . . will require complete good faith on the part of the belligerents, as well as the desire to conform with the general principle of respect for the civilian population."[86]

Further complicating matters is the issue of reverberating effects, i.e., those effects not directly and immediately caused by the attack, but nevertheless the product thereof—it is the problem of the effects caused by the effects of an attack. The most cited example involves the attack on the Iraqi electrical grid during the 1991 Persian Gulf War. Although it successfully disrupted Iraqi command and control, the attack also denied electricity to the civilian population (a "first-tier" effect), thereby affecting hospitals, refrigeration, emergency response, etc. Similarly, when NATO struck at Yugoslavia's electrical supply network during Operation ALLIED FORCE, one consequence was shutting down drinking water pumping stations.[87] Such attacks set off "second-tier" suffering (a reverberating effect) of the population. Obviously, precisely the

same effects could have resulted had the attacks been conducted through CNA. Indeed, the problem of reverberating effects looms much larger in computer network than kinetic attacks due to the interconnectivity of computers, particularly that between military and civilian systems.

Reverberating effects bear on proportionality analysis because they must be considered when balancing collateral damage and incidental injury against military advantage. Unfortunately, and whether reverberating or direct, it is difficult to assess such damage and injury when caused by computer network attack absent an understanding of how the computer systems involved function and to which other systems they are linked. Despite this obstacle, planners and decision-makers have an affirmative duty to attempt to avoid collateral damage and incidental injury whenever feasible, a duty that necessarily implies an effort to ascertain the resultant damage or injury from an attack.[88] Given the complexity of computer network attack, the high likelihood of an impact on civilian systems, and the relatively low understanding of its nature and effects on the part of those charged with ordering the attacks, computer experts will have to be available to assess potential collateral and incidental effects throughout the mission planning process.[89] Additionally, modeling and simulation, like that already conducted for nuclear weapons, would prove invaluable in identifying possible reverberating effects; conducting them prior to the outbreak of hostilities—free from the fog, friction, and pace of war—would be well advised.

Minimizing collateral damage and incidental injury: Proportionality determinations establish whether a military objective may be attacked at all. However, even if the selected target is legitimate and the planned attack thereon would be proportional, the attacker has an obligation to select that method or means of warfare likely to cause the least collateral damage and incidental injury, all other things being equal (such as risk to the forces conducting the attack, likelihood of success, weapons inventory, etc.).[90] Additionally, whenever a choice is presented between military objectives that can be attacked to achieve a desired result, the attack which risks the least collateral damage and incidental injury must be chosen.[91]

The availability of computer network attack actually expands the options for minimizing collateral damage and incidental injury. Whereas in the past physical destruction may have been necessary to neutralize a target's contribution to the enemy's efforts, now it may be possible to simply "turn it off." For instance, rather than bombing an airfield, air traffic control can be interrupted. The same is true of power production and distribution systems, communications, industrial plants, and so forth. Those who plan and execute such operations must still be concerned about collateral damage, incidental injury, and reverberating

effects (consider the Iraqi electric grid example *supra*), but the risks associated with conducting classic kinetic warfare are mitigated significantly through CNA. Additionally, depending on the desired result, it may be possible to simply interrupt operation of the target. This tactic would be particularly attractive in the case of dual-use objectives. Consider an electrical grid. It might only be militarily necessary to shut the system down for a short period, for example, immediately preceding and during an assault. The system could be brought back up as soon as the pressing need for its interruption passed, thereby limiting the negative effects on the civilian population. Along the same lines, because targets are not physically damaged, and thus do not need to be repaired or rebuilt, the civilian population's return to normalcy at the end of the conflict would be facilitated.

There is, from a humanitarian point of view, one theoretical downside to the fact that CNA may sometimes cause less collateral damage and incidental injury than kinetic attacks—it might actually encourage attacks. This would be so in the case of an attack that could not pass the proportionality test if conducted kinetically, but could if accomplished by computer network attack. Should the CNA result in any collateral damage or incidental injury (albeit not enough to outweigh the resulting military advantage), the net result would be greater civilian suffering. While this is true, the better question from the humanitarian point of view is whether CNA causes more or less collateral damage and incidental injury overall, not merely as to a single operation. So long as the various limitations of the principle of discrimination are complied with, and without the benefit of a track record to draw on in making the assertion, it would seem that in humanitarian terms computer network attack is probably a step forward.

Perfidy: Although the core normative constraints on computer network attack derive from the principle of discrimination, several other related aspects of humanitarian law are implicated by this new means of warfare. One is the prohibition on perfidy. Perfidy is the feigning of protected status in order to take advantage of an adversary. Examples include pretending to be wounded or sick, to enjoy non-combatant status, or to surrender, and improperly displaying symbols that signify protected status, such as the red cross or red crescent. Perfidy is distinguished from ruses, which are acts intended to mislead an adversary and cause him to act recklessly, but which do not involve false claims of protected status. Ruses are lawful.

Information warfare, including computer network attack, opens many opportunities for ruses and perfidy. This is because both techniques are intended to convey false information. For instance, lawful ruses might include transmitting false data, meant to be intercepted by an adversary, regarding troop disposition

or movements. Alternatively, it might involve altering data in an adversary's intelligence databases, sending messages to enemy headquarters purporting to be from subordinate units, or passing instructions to subordinate units that appear to be from their headquarters.[92] All such activities would be perfectly legitimate.

On the other hand, any action intended to mislead the enemy into believing that one's forces enjoyed protected status in order to kill, injure, or capture the enemy would be illegitimate.[93] For instance, medical units and transports may use codes and signals established by the International Telecommunications Union, the International Civil Aviation Organization, and the International Maritime Consultative Organization to identify themselves.[94] Falsely transmitting such code/signals or, a more likely prospect in the computer network attack context, causing adversary systems to reflect receipt of such signals would be clear examples of perfidy. The Department of Defense has also opined that using "computer 'morphing' techniques to create an image of the enemy's chief of state informing his troops that an armistice or cease-fire agreement had been signed" would be a war crime if false.[95]

An interesting prospect would be routing a computer network attack through civilian systems, or otherwise feigning a civilian source. This might be done to later mask the source of attack or to inspire confidence in the target that the transmission was benign. Doing so would be prohibited both by the Protocol Additional I and customary law.[96] This is a very sensible restriction because a response to an attack apparently originating from a civilian source could be kinetic in nature.

It must be noted that the protocol's restriction on perfidy is limited to conduct calculated to facilitate killing, injuring, or capturing an adversary. The commentary thereto notes this limitation, but suggests that "there is more to an international treaty than the literal reading of all the words in the document may suggest; it represents one step forward in the ongoing evolution in relations between States."[97] Be that as it may, as the law stands today it would be permissible to disguise information warfare operations as civilian in origin if they were not related to killing, injuring, or capturing one's adversary. This standard is consistent with that employed *supra* regarding "armed" conflict and "attack." Moreover, the prohibition on misuse of protective codes and signals, such as those designed to identify medical facilities, are absolute, i.e., they apply regardless of the abuser's intent. As an example, usage merely to avoid attack is forbidden.

Civilian Shields: In theory, a computer attack might utilize a civilian network to shield itself against a response, either kinetic or through a counter-cyber attack. If the latter did not cause death or injury to civilians or damage

or destruction of protected objects, and therefore was not an "attack" in the humanitarian law sense, it would be permissible. On the other hand, if it might cause collateral damage or incidental injury, then any such effects on the civilian population would have to be considered in a proportionality analysis; civilians and civilian objects do not lose the protections of the law of armed conflict by the wrongful acts of others. Of course, the use of civilian shields is itself wrongful;[98] the party that subjects the civilian population or protected objects to risk by using them as shields is culpable under humanitarian law. This principle applies whether the attack is kinetic or computer in nature.

Mercenaries: Since computer network attacks can amount to both armed conflict and, in individual cases, an attack, restrictions on mercenaries may apply to those who conduct them. Mercenaries are specifically addressed in Protocol Additional I, although the restrictions contained therein are not customary in nature, a position strengthened by the absence of any mention of mercenaries in the Statute of the International Criminal Court.

By Article 47 of the protocol, a mercenary is any person who:

> (a) is specially recruited locally or abroad in order to fight in an armed conflict;
> (b) does, in fact, take a direct part in the hostilities;
> (c) is motivated to take part in the hostilities essentially by the desire for private gain and, in fact, is promised, by or on behalf of a Party to the conflict, material compensation substantially in excess of that promised or paid to combatants of similar ranks and functions in the armed forces of that Party;
> (d) is neither a national of a Party to the conflict nor a resident of territory controlled by a Party to the conflict;
> (e) is not a member of the armed forces of a Party to the conflict; and
> (f) has not been sent by a State which is not a Party to the conflict on official duty as a member of its armed forces.[99]

While Protocol Additional I does not actually prohibit mercenarism, because they are not combatants, mercenaries are not entitled to prisoner of war status. Therefore, like any other noncombatant who directly engages in hostilities, they may be tried under the domestic law of the State that captures them.[100]

Given the complexity of conducting computer network attacks, it is quite conceivable that States might hire non-nationals possessing the requisite expertise to mount them. If the CNA amount to an "attack," these individuals would be taking a "direct part in the hostilities." Assuming they met the other qualifying criteria for mercenaries, the Protocol Additional I provisions would apply. Interestingly, there is a financial incentive to outsource CNA because in

many cases hiring computer attack expertise would be far more cost-effective than hiring conventional attack mercenaries or even acquiring weapons for one's own forces.

Conclusion

By and large, as information warfare capabilities increase, existing humanitarian prescriptive norms will suffice to maintain the protection civilians, civilian objects, and other protected entities enjoy. However, certain novel aspects of CNA do pose new and sometimes troubling quandaries. The unease over the use of cyber warfare during NATO's campaign against Yugoslavia in 1999 is compelling evidence that the question of how humanitarian law bears on CNA remains unsettled.[101]

First, in order to apply extant norms to CNA, it is necessary to accept various interpretive premises. Most important are the consequence-based interpretations of "armed conflict" and "attack." Absent such understandings, the applicability, and therefore adequacy, of present-day humanitarian law principles would fall into question. Interestingly, consideration of computer network attack in the context of the *jus ad bellum* also leads to consequence-based interpretation.[102]

Second, even accepting the parameters resulting from the interpretations suggested, normative lacunae exist. Most notably, attacks against civilians and civilian objects that do not injure, kill, damage, or destroy (or otherwise produce the requisite level of suffering) are by and large permissible. Given that kinetic attacks usually have such effects, civilians and civilian objects enjoy broad protection during conventional military operations. However, computer network attack, because it may not amount to an *attack,* opens up many possibilities for targeting otherwise protected persons and objects. The incentive for conducting such operations grows in relation to the extent to which the "war aims" of the party conducting the CNA are coercive in nature; the desire to, e.g., "turn out the lights" to a civilian population in order motivate it to pressure its leadership to take, or desist from taking, a particular course of conduct (a step suggested by NATO's air commander during Operation ALLIED FORCE) will grow as the means for doing so expand.[103] This is an especially negative reality in humanitarian terms.

Third, and more encouraging, is the fact that CNA may make it possible to achieve desired military objectives with less collateral damage and incidental injury than in traditional kinetic attacks. Indeed, in certain cases, military commanders will be obligated to employ their cyber assets in lieu of kinetic weapons

when collateral and incidental effects can be limited.[104] That said, it will be critically important to carefully analyze the effects of such operations, particularly their reverberating effects, when assessing an attack's compliance with the principle of proportionality. This will require planning, legal, and computer experts to operate in concert throughout the targeting cycle.[105]

Finally, much as CNA challenges existing notions of "attack," it will also test traditional understanding of combatant status. This results from the use of typically civilian technology and know-how to conduct military operations via computer. Failure to strictly comply with the limitations on the participation of civilians in hostilities will inevitably lead to heightened endangerment of the civilian population and weaken humanitarian law norms.

So the jury remains out. While humanitarian law in its present form generally suffices to safeguard those it seeks to protect from the effects of computer network attack, and even though it offers the promise of periodically enhancing such protection, significant prescriptive fault lines do exist. Thus, as capabilities to conduct computer network attacks increase, both in terms of sophistication and availability, continued normative monitoring is absolutely essential. We must avoid losing sight of humanitarian principles, lest the possible in warfare supplant the permissible.

Notes

* An abbreviated version of this chapter appears in the *International Review of the Red Cross* (2002) edition commemorating the 25th anniversary of the Protocols Additional.

1. The United States National Military Strategy cites information superiority as a key element of its strategy for this century. "Information superiority is the capability to collect, process, and disseminate an uninterrupted flow of precise and reliable information, while exploiting and denying an adversary's ability to do the same." Chairman of the Joint Chiefs of Staff, National Military Strategy, (1997), www.dtic.mil/jcs/nms/strategy.htm, at n.p. For an excellent collection of essays on the nature of war in the 21st century, see FUTURE WARFARE ANTHOLOGY (Robert H. Scales ed., 2000). On the specific issue of information and conflict, see STEVEN METZ, ARMED CONFLICT IN THE 21ST CENTURY: THE INFORMATION REVOLUTION AND POST-MODERN WARFARE (2000); WILLIAM A. OWENS & EDWARD OFFLEY, LIFTING THE FOG OF WAR (2000); THE INFORMATION REVOLUTION AND NATIONAL SECURITY (Thomas E. Copeland ed., 2000); DAVID S. ALBERTS, JOHN J. GARSTKA & FREDERICK P. STEIN, NETWORK CENTRIC WARFARE: DEVELOPING AND LEVERAGING INFORMATION SUPERIORITY (1999); DAN KUEHL, STRATEGIC INFORMATION WARFARE: A CONCEPT (1999); THE CHANGING ROLE OF INFORMATION WARFARE (Zalmay Khalilzad & John White eds., 1999); DOROTHY E. DENNING, INFORMATION WARFARE AND SECURITY (1998); JAMES ADAMS, THE NEXT WORLD WAR: COMPUTERS ARE THE WEAPONS AND THE FRONT LINE IS EVERYWHERE (1998).

2. Chairman of the Joint Chiefs of Staff, Department of Defense Dictionary of Military and Associated Terms, Joint Publication 1-02, April 12, 2001, at 203 [hereinafter Joint Pub 1-02]. Operations that might constitute information operations include operations security,

psychological operations, military deception, electronic warfare, physical attack, and computer network attack. *See* Chairman of the Joint Chiefs of Staff, Joint Publication 3-13, Joint Doctrine for Information Operations, at I-9, (1998) [hereinafter Joint Pub 3-13].

3. At the strategic level, IO can be employed to "achieve national objectives by influencing or affecting all elements (political, military, economic, or informational) of an adversary's or potential adversary's national power while protecting similar friendly elements." At the operational level, the focus of IO is "on affecting adversary lines of communication (LOCs), logistics, command and control (C2), and related capabilities and activities while protecting similar friendly capabilities and activities." Finally, at the tactical level the objective is to affect adversary "information and information systems relating to C2, intelligence, and other information-based processes directly relating to the conduct of military operations. . . ." Joint Pub 3-13, *supra* note 2, at I-2–I-3.

4. Joint Pub 1-02, *supra* note 2, at 203.

5. *Id.* at 88. The USAF Intelligence Targeting Guide, AF Pamphlet 14-210, Feb, 1, 1998, para. 11.4.3, notes IW employment concepts:

> Corruption – The alteration of information content; the manipulation of data to make it either nonsensical or inaccurate. Destroying existing knowledge.
>
> Deception – A specific type of corruption; the alteration of, or adding to, information to portray a situation different from reality. Creating false knowledge to include masquerading.
>
> Delay – The reversible slowing of the flow of information through the system, and the slowing of the acquisition and dissemination of new knowledge.
>
> Denial – The reversible stopping of the flow of information for a period of time; although the information may be transmitted and used within friendly territory, the adversary is denied access to it. The prevention of the acquisition and dissemination of new knowledge.
>
> Disruption – The reduction of the capacity to provide and/or process information (reversible). This is a combination of delay and corruption. The delay of the acquisition and dissemination of new knowledge and the destruction of existing knowledge.
>
> Degradation – The permanent reduction in the capacity to provide and/or process information.
>
> Destruction – The destruction of information before it can be transmitted; the permanent elimination of the capacity to provide and/or process information.

6. Thus, electronic attack (EA) would not fall within this category. For instance, using an electromagnetic pulse to destroy a computer's electronics would be EA, whereas transmitting a code or instruction to a system's central processing unit to cause the power supply to short out would be CNA. *Id.*

7. On CNA and the *jus ad bellum*, that body of international law governing the legality of the resort to force by States, see Michael N. Schmitt, *Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework*, 37 COLUMBIA JOURNAL OF TRANSNATIONAL LAW 885 (1999); Richard Aldrich, *How Do You Know You are at War in the Information Age?*, 22 HOUSTON JOURNAL OF INTERNATIONAL LAW 223 (2000).

8. For a discussion of CNA in the context of both law and ethics that concludes a new convention is required, see William J. Bayles, *The Ethics of Computer Network Attack*, PARAMETERS, Spring 2001, at 44.

9. On this point see Emily Haslam, *Information Warfare: Technological Changes and International Law*, 5 JOURNAL OF CONFLICT AND SECURITY LAW 157 (2000), particularly her discussion of points made in Richard Aldrich, *The International Legal Implications of Information Warfare*,

AIRPOWER JOURNAL, Fall 1996, at 99, and Mark Shulman, *Discrimination in the Laws of Information Warfare*, 37 COLUMBIA JOURNAL OF TRANSNATIONAL LAW 939 (1999).

10. Hague Convention IV Respecting the Laws and Customs of War on Land, Oct. 18, 1907, pmbl., 36 Stat. 2295, 1 Bevans 634, reprinted in ADAM ROBERTS & RICHARD GUELFF, DOCUMENTS ON THE LAWS OF WAR 67 (3d ed. 2000); Protocol Additional (I) to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts, art. 1(2), Dec. 12, 1977, 1125 U.N.T.S. 3, 16 INTERNATIONAL LEGAL MATERIALS 1391 (1977), *reprinted in* ROBERTS & GUELFF, *supra*, at 419 [hereinafter Protocol Additional I].

11. The Statute of the International Court of Justice defines custom as "a general practice accepted by law." Statute of the International Court of Justice, June 26, 1977, art. 38(1)(b), 59 Stat. 1031, T.S. No. 933, 3 Bevans 1153, 1976 Y.B.U.N. 1052. The Restatement notes that custom "results from a general and consistent practice of states followed by them from a sense of legal obligation." Restatement (Third), Foreign Relations Law of the United States, sec. 102(2) (1987). See also North Sea Continental Shelf Cases, 1969 I.C.J. 3, 44 ("Not only must the acts concerned amount to settled practice, but they must also be such, or be carried out in such a way, as to be evidence of a belief that this practice is rendered obligatory by the existence of a rule requiring it."); The Paquete Habana, 175 US 677, 20 S.Ct. 290, 44 L.Ed 320 (1900); The Case of the S.S. Lotus (Fr. v. Turk.), 1927 P.C.I.J. (ser. A) No. 10(1927); Asylum Case (Col. v. Peru), 1950 I.C.J. 266; Case Concerning Right of Passage over Indian Territory (Port. v. India), 1960 I.C.J. 6. For academic comment on customary international law, see Jack L. Goldsmith & Eric A. Posner, *Understanding the Resemblance Between Modern and Traditional Customary International Law*, 40 VIRGINIA JOURNAL OF INTERNATIONAL LAW 639 (2000); Patrick Kelly, *The Twilight of Customary International Law*, 40 VIRGINIA JOURNAL OF INTERNATIONAL LAW 449 (2000); ANTHONY A. D'AMATO, THE CONCEPT OF CUSTOM IN INTERNATIONAL LAW (1971).

12. Legality of the Threat or Use of Nuclear Weapons (Advisory Opinion), 1996 I.C.J. 226 (July 8), 35 INTERNATIONAL LEGAL MATERIALS 809, para. 85.

13. Protocol Additional I, *supra* note 10, art. 36: "In the study, development, acquisition or adoption of new weapons, means or methods of warfare, a High Contracting Party is under an obligation to determine whether its employment would, in some or all circumstances, be prohibited by this Protocol or by any other rule of international law applicable to the High Contracting Party." For the United States, the weapon review is required by Department of Defense Instruction 5000.2, Operation of the Defense Acquisition System, Oct. 23, 2000, para. 4.7.3.1.4. It provides, in relevant part, that "DoD acquisition and procurement of weapons and weapon systems shall be consistent with all applicable domestic law and all applicable treaties, customary international law, and the law of armed conflict (also known as the laws and customs of war) . . . . Additionally, legal reviews of new, advanced or emerging technologies that may lead to development of weapons or weapon systems are encouraged."

14. For instance, see the analysis in Robert G. Hanseman, *The Realities and Legalities of Information Warfare*, 42 AIR FORCE LAW REVIEW 173, 183–184 (1997).

15. *See generally*, Schmitt, *supra* note 7.

16. *See generally*, contributions to *Symposium: The International Legal Fallout from Kosovo*, 12 EUROPEAN JOURNAL OF INTERNATIONAL LAW 391 (2001); Bruno Simma, *NATO, the UN and the Use of Force: Legal Aspects*, 10 EUROPEAN JOURNAL OF INTERNATIONAL LAW 1 (1999); Antonio Cassese, *Ex iniuria ius oritur: Are We Moving towards International Legitimation of Forcible Humanitarian Countermeasures in the World Community*, 10 EUROPEAN JOURNAL OF INTERNATIONAL LAW 23 (1999).

17. For a description of Russian actions, see Human Rights Watch, World Report 2001 (Russia), www.hrw.org/wr2k1. The abuses were condemned in UN Commission on Human

Rights Resolution 2001/24, Situation in the Republic of Chechnya of the Russian Federation, UN Doc. E/CN.4/RES/2001/24, April 20, 2001.

18. LESLIE C. GREEN, THE CONTEMPORARY LAW OF ARMED CONFLICT 70 (2d ed. 2000).

19. Geneva Convention for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field, Aug. 12, 1949, art. 2, 6 U.S.T. 3114, 75 U.N.T.S. 31 [hereinafter GC I]; Geneva Convention for the Amelioration of the Condition of the Wounded, Sick and Shipwrecked Members of the Armed Forces at Sea, Aug. 12, 1949, art. 2, 6 U.S.T. 3217, 75 U.N.T.S. 85 [hereinafter GC II]; Geneva Convention Relative to the Treatment of Prisoners of War, Aug. 12, 1949, art. 2, 6 U.S.T. 3316, 75 U.N.T.S. 135 [hereinafter GC III]; and Geneva Convention Relative to the Protection of Civilian Persons in Time of War, Aug. 12, 1949, art. 2, 6 U.S.T. 3516, 75 U.N.T.S. 287 [hereinafter GC IV] (emphasis added). The conventions are *reprinted in* ROBERTS & GUELFF, *supra* note 10, at 195, 221, 243, and 249 respectively.

20. Protocol Additional I, *supra* note 10, art. 1.

21. Protocol Additional (II) to the Geneva Conventions of August 12, 1949, and Relating to the Protection of Victims of Non-international Armed Conflicts, June 8, 1977, 1125 U.N.T.S. 609, 16 INTERNATIONAL LEGAL MATERIALS 1442 (1977), *reprinted in* ROBERTS & GUELFF, *supra* note 10, at 481.

22. Protocol Additional I deals with conflict between States, whereas Protocol Additional II is that between a State and a rebel group (or groups).

23. Non-international armed conflict can occur solely within the confines of a single State.

24. Hague Convention (III) Relative to the Opening of Hostilities, Oct. 18, 1907, art. 1, 1 Bevans 619, 2 AMERICAN JOURNAL OF INTERNATIONAL LAW (Supp.) 85 (1908), *reprinted in* DIETRICH SCHINDLER & JIRI TOMAN, THE LAWS OF ARMED CONFLICT 57 (1988). According to the commentary to the 1949 Geneva Conventions, "[t]here is no longer any need for a formal declaration or war, or for recognition of the state of war, as preliminaries to the application of the Convention. The Convention becomes applicable as from the actual opening of hostilities." COMMENTARY: GENEVA CONVENTION FOR THE AMELIORATION OF THE CONDITION OF THE WOUNDED AND SICK IN ARMED FORCES IN THE FIELD 32 (Jean Pictet ed., 1952) [hereinafter GC I COMMENTARY].

25. GC I COMMENTARY, *supra* note 24, at 32–33 (emphasis added).

26. COMMENTARY ON THE ADDITIONAL PROTOCOLS OF 8 JUNE 1977 TO THE GENEVA CONVENTIONS OF 12 AUGUST 1949, para. 62 (emphasis added) (Yves Sandoz, Christophe Swinarki & Bruno Zimmerman eds., 1987) [hereinafter PROTOCOLS ADDITIONAL COMMENTARY]. The commentary to Protocol Additional II refers back to the commentary to common Article 3 of the 1949 Conventions and to that on Protocol Additional I. *Id.*, para. 4448, fn 2.

27. PROTOCOLS ADDITIONAL COMMENTARY, *supra* note 26, para. 4341 (emphasis added).

28. *See, e.g.*, discussion in INGRID DETTER, THE LAW OF WAR 20–21 (2d ed. 2000); Christopher Greenwood, *Historical Development and Legal Basis*, *in* THE HANDBOOK OF HUMANITARIAN LAW IN ARMED CONFLICT 1, 42 (Dieter Fleck ed., 1995).

29. For instance, the Preamble to Protocol Additional I notes that "it [is] necessary . . . to reaffirm and develop the provisions protecting the victims of armed conflicts and to supplement measures intended to reinforce their application." Additional Protocol I, *supra* note 10, pmbl.

30. The designation "Geneva Law" refers to that portion of the law of armed conflict addressing protected classes of persons: civilians, prisoners of war, the sick or shipwrecked, and medical personnel. It is distinguished from "Hague Law," which governs methods and means of combat, occupation, and neutrality. For a discussion of the international instruments which fall into each category, and of those which display elements of both, see FREDERIC DEMULINEN, HANDBOOK ON THE LAW OF WAR FOR ARMED FORCES 3-4 (1987).

31. On the topic of attribution of an act to a State, see the International Law Commission's Draft Articles on State Responsibility, 1996 ILC Report, ch. III, www.un.org/law/ilc/reports/1996/chap03.htm#doc38.

32. This possibility was described in PRESIDENT'S COMMISSION ON CRITICAL INFRASTRUCTURE PROTECTION, CRITICAL FOUNDATIONS: PROTECTING AMERICA'S INFRASTRUCTURES, Oct. 1997, at A-46.

33. Although not a Party to Protocol Additional I, the United States considers many of its provisions to be declaratory of customary international law. For a non-official, but generally considered authoritative, delineation of those viewed as declaratory, see Michael J. Matheson, *Session One: The United States Position on the Relation of Customary International Law to the 1977 Protocols Additional to the 1949 Geneva Conventions*, 2 AMERICAN UNIVERSITY JOURNAL OF INTERNATIONAL LAW AND POLICY 419 (1987). *See also* INTERNATIONAL & OPERATIONAL LAW DIVISION, OFFICE OF THE JUDGE ADVOCATE GENERAL, DEPARTMENT OF THE AIR FORCE, OPERATIONS LAW DEPLOYMENT DESKBOOK, tab 12, no date, and comments by the then State Department Legal Advisor Abraham D. Soafer in *Agora: The US Decision Not to Ratify Protocol I to the Geneva Conventions on the Protection of War Victims*, 82 AMERICAN JOURNAL OF INTERNATIONAL LAW 784 (1988).

34. Protocol Additional I, *supra* note 10, art. 48. The centrality of the principle to humanitarian law is noted in the ICRC commentary thereon:

> The basic rule of protection and distinction is confirmed in this article. It is the foundation on which the codification of the laws and customs of war rests: the civilian population and civilian objects must be respected and protected in armed conflict, and for this purpose they must be distinguished from combatants and military objectives. The entire system established in The Hague in 1899 and 1907 and in Geneva from 1864 to 1977 is founded on this rule of customary law. It was already implicitly recognized in the St. Petersburg Declaration of 1868 renouncing the use of certain projectiles, which had stated that "the only legitimate object which States should endeavour to accomplish during war is to weaken the military forces of the enemy." Admittedly this was concerned with preventing superfluous injury or unnecessary suffering to combatants by prohibiting the use of all explosive projectiles under 400 grammes in weight, and was not aimed at specifically protecting the civilian population. However, in this instrument the immunity of the population was confirmed indirectly.
>
> In the Hague Conventions of 1899 and 1907, like the Geneva Conventions of 1929 and 1949, the rule of protection is deemed to be generally accepted as a rule of law, though at that time it was not considered necessary to formulate it word for word in the texts themselves. The rule is included in this Protocol to verify the distinction required and the limitation of attacks on military objectives.

PROTOCOLS ADDITIONAL COMMENTARY, *supra* note 26, paras. 1863–64.

35. Protocol Additional I, *supra* note 10, art. 51.2.

36. *Id.*, art. 52.1.

37. *Id.*, art. 51.4.

38. *Id.*, art. 52.2.

39. *Id.*, arts. 51.1 & 51.2 (emphasis added).

40. PROTOCOLS ADDITIONAL COMMENTARY, *supra* note 26, para. 1875 (emphasis added).

41. It is reasonable to include human suffering in the meaning based on the fact that the protocol prohibits causing terror, also a mental condition. Protocol Additional I, *supra* note 10, art. 51.2.

42. *Id.*, arts. 51.5(b); 57.2(a)(iii); 57.2(b).

43. *Id.*, arts. 35.3 & 55.1.

44. *Id.*, art. 56.1.

45. PROTOCOLS ADDITIONAL COMMENTARY, *supra* note 26, para. 1881.

46. *But see* Haslam, *supra* note 9, at 173.

47. Indeed, the United States has even developed doctrine for the conduct of psychological operations. Chairman of the Joint Chiefs of Staff, Joint Doctrine for Psychological Operations, Joint Publication 3-53, July 10, 1996. Actions intended to terrorize the civilian population are prohibited by Protocol Additional I, *supra* note 10, art. 51.2.

48. Protocol Additional I, *supra* note 10, art. 57.2(a)(i). The commentary to the provision further explains the obligation.

> Admittedly, those who plan or decide upon such an attack will base their decision on information given them, and they cannot be expected to have personal knowledge of the objective to be attacked and of its exact nature. However, this does not detract from their responsibility, and in case of doubt, even if there is only slight doubt, they must call for additional information and if need be give orders for further reconnaissance to those of their subordinates and those responsible for supportive weapons (particularly artillery and air force) whose business this is, and who are answerable to them. In the case of long-distance attacks, information will be obtained in particular from aerial reconnaissance and from intelligence units, which will of course attempt to gather information about enemy military objectives by various means. The evaluation of the information obtained must include a serious check of its accuracy, particularly as there is nothing to prevent the enemy from setting up fake military objectives or camouflaging the true ones. In fact it is clear that no responsible military commander would wish to attack objectives which were of no military interest. In this respect humanitarian interests and military interests coincide.

PROTOCOLS ADDITIONAL COMMENTARY, *supra* note 26, para. 2195.

49. Protocol Additional I, *supra* note 10, art. 43.1–2.

50. *Id.*, art. 52.2.

51. Indeed, the commentary states that: "The text of this paragraph certainly constitutes a valuable guide, but it will not always be easy to interpret, particularly for those who have to decide about an attack and on the means and methods to be used." PROTOCOLS ADDITIONAL COMMENTARY, *supra* note 26, para. 2016.

52. *Id.*, paras. 2020–23.

53. *Id.*, para. 2024.

54. US Navy/Marine Corps/Coast Guard, The Commander's Handbook on the Law of Naval Operations (NWP 1-14M, MCWP 5-2.1, COMDTPUB P5800.7), para 8.1.1 (1995), *reprinted in* its annotated version as Volume 73 of the US Naval War College's International Law Studies series [hereinafter Handbook]. This assertion is labeled a "statement of customary international law." The Handbook cites General Counsel, Department of Defense, Letter of Sept. 22, 1972, *reprinted in* 67 AMERICAN JOURNAL OF INTERNATIONAL LAW 123 (1973), as the basis for this characterization.

55. Bankovic & Others v. Belgium, the Czech Republic, Denmark, France, Germany, Greece, Hungary, Iceland, Italy, Luxembourg, the Netherlands, Norway, Poland, Portugal, Spain, Turkey and the United Kingdom.

56. Protocol Additional I, *supra* note 10, art. 50.1.

57. *Id.*, art. 52.1.

58. *Id.*, art. 51.2 & 52. The Statute for the International Criminal Court also prohibits the direct targeting of civilians or civilian objects. Rome Statute for the International Criminal Court, art. 8.2(b)(i) & (ii), U.N. Doc. A/Conf. 183/9, July 17, 1998, at Annex II [hereinafter Rome Statute], *reprinted in* 37 INTERNATIONAL LEGAL MATERIALS 999 (1998), and M. CHERIF BASSIOUNI,

THE STATUTE OF THE INTERNATIONAL COURT: A DOCUMENTARY HISTORY 39 (1999), and available on-line at www.un.org/law/icc/texts/romefra.htm.

59. *Id.*, arts. 50.1 (for civilians) & 52.3 (for civilian objects).

60. *Id.*, art. 51.3; PROTOCOLS ADDITIONAL COMMENTARY, *supra* note 26, para. 1944.

61. Letter from DAJA-IA to Counselor for Defense Research and Engineering (Economics), Embassy of the Federal Republic of Germany (Jan. 22, 1988), *cited in* W.H. Parks, *Air War and the Law of War*, 32 AIR FORCE LAW REVIEW 1, 34 (1992).

62. GC III, *supra* note 19, art. 4(4).

63. *Id.*

64. Protocol Additional I, *supra* note 10, art. 56.1. This prohibition extends to attacks on other military objectives in their vicinity if the attack might cause such a release. There are exceptions to the general prohibition of the article.

> 2. The special protection against attack provided by paragraph 1 shall cease:
> (a) for a dam or a dyke only if it is used for other than its normal function and in regular, significant and direct support of military operations and if such attack is the only feasible way to terminate such support;
> (b) for a nuclear electrical generating station only if it provides electric power in regular, significant and direct support of military operations and if such attack is the only feasible way to terminate such support;
> (c) for other military objectives located at or in the vicinity of these works or installations only if they are used in regular, significant and direct support of military operations and if such attack is the only feasible way to terminate such support.

Id., art. 56.2.

65. *Id.*, art. 54.2. See also Rome Statute, *supra* note 58, art. 8.2(b)(xxv).

66. PROTOCOLS ADDITIONAL COMMENTARY, *supra* note 26, para. 2110. However, the prohibition does not apply to objects used solely for the sustenance of enemy forces or "in direct support of military action." Protocol Additional I, *supra* note 10, art. 54.3. An example of the latter would be a agricultural area used for cover by military forces.

67. *Id.*, arts. 35.3 & 55. See also Rome Statute, *supra* note 58, art. 8.2(b)(iv). On the issue of environmental damage during armed conflict, see THE ENVIRONMENTAL CONSEQUENCES OF WAR: LEGAL, ECONOMIC, AND SCIENTIFIC PERSPECTIVES (Jay E. Austin & Carl E Bruch eds., 2000); Michael N. Schmitt, *Green War: An Assessment of the Environmental Law of International Armed Conflict*, 22 YALE JOURNAL OF INTERNATIONAL LAW 1-109 (1997); PROTECTION OF THE ENVIRONMENT DURING ARMED CONFLICT AND OTHER MILITARY OPERATIONS (Richard J. Grunawalt, John E. King & Ronald S. McClain eds., 1996) (Vol. 69, US Naval War College International Law Studies).

68. Protocol Additional I, *supra* note 10, art. 12. However, note that there are specific criteria for the extension of protection to civilian facilities. *Id.*, art. 12.2. See also Rome Statute, *supra* note 58, art. 8.2(b)(ix) & (xxv).

69. *Id.*, arts. 21–31. The extent of the protection varies depending on the category of transportation and its location.

70. *Id.*, art. 53.

71. *Id.*, art. 62.3.

72. *Id.*, art. 70. Special provisions as to when such operations are entitled to the protection apply. Rome Statute, *supra* note 58, art. 8.2(b)(iii).

73. GC I, *supra* note 19, art. 46; GC II, *supra* note 19, art. 47; GC III, *supra* note 19, art. 13; GC IV, *supra* note 19, art. 33; Protocol Additional I, *supra* note 10, arts. 20, 51–56.

74. An example of an attack on a combatant that would be unlawful is one that employs a forbidden weapon, such as poison.

75. Soafer, *supra* note 33, at 470. For the official US position on reprisals against civilians, see Handbook, *supra* note 54, paras. 6.2.3 & 6.2.3.1–3.

76. The reservation reads:

> The obligations of Articles 51 and 55 are accepted on the basis that any adverse party against which the United Kingdom might be engaged will itself scrupulously observe those obligations. If an adverse party makes serious and deliberate attacks, in violation of Article 51 or Article 52 against the civilian population or civilians or against civilian objects, or, in violation of Articles 53, 54 and 55, on objects or items protected by those Articles, the United Kingdom will regard itself as entitled to take measures otherwise prohibited by the Articles in question to the extent that it considers such measures necessary for the sole purpose of compelling the adverse party to cease committing violations under those Articles, but only after formal warning to the adverse party requiring cessation of the violations has been disregarded and then only after a decision taken at the highest level of government. Any measures thus taken by the United Kingdom will not be disproportionate to the violations giving rise there to and will not involve any action prohibited by the Geneva Conventions of 1949 nor will such measures be continued after the violations have ceased. The United Kingdom will notify the Protecting Powers of any such formal warning given to an adverse party, and if that warning has been disregarded, of any measures taken as a result.

Reprinted on the International Committee of the Red Cross Treaty Database website, www.icrc.org/ihl.

77. For a comprehensive review of the principle, see ESBJÖRN ROSENBLAD, INTERNATIONAL HUMANITARIAN LAW OF ARMED CONFLICT: SOME ASPECTS OF THE PRINCIPLE OF DISTINCTION AND RELATED PROBLEMS (1979).

78. This typology is adopted from Christopher Greenwood, *The Law of Weaponry at the Start of the New Millennium*, in THE LAW OF ARMED CONFLICT: INTO THE NEXT MILLENNIUM 185 (Michael N. Schmitt & Leslie C. Green eds., 1998) (Vol. 71, US Naval War College International Law Studies). By contrast, the US Air Force employs the categories of military necessity, humanity, and chivalry, with proportionality folded into necessity, whereas the US Navy uses necessity, humanity and chivalry. *Compare* DEPARTMENT OF THE AIR FORCE, INTERNATIONAL LAW—THE CONDUCT OF ARMED CONFLICT AND AIR OPERATIONS (AF Pamphlet 110-31, 1976), at 1-5–1-6 with Handbook, *supra* note 54, para. 5-1.

79. PROTOCOLS ADDITIONAL COMMENTARY, *supra* note 26, para. 1957.

80. On the attacks, see U.S. DEPARTMENT OF DEFENSE, CONDUCT OF THE PERSIAN GULF WAR (Title V Report to Congress) (1992), at 623, *reprinted in* 31 INTERNATIONAL LEGAL MATERIALS 612 (1992).

81. An expanded discussion is in Michael N. Schmitt, *Bellum Americanum: The US View of Twenty-First Century War and its Possible Implications for the Law of Armed Conflict*, 19 MICHIGAN JOURNAL OF INTERNATIONAL LAW 1051, 1080–81 (1998).

82. Protocol Additional I, *supra* note 10, arts. 51.5(a) & 57.2(a)(iii) & (b). On proportionality, see William J. Fenrick, *The Rule of Proportionality and Protocol Additional I in Conventional Warfare*, 98 MILITARY LAW REVIEW 91 (1982); Judith G. Gardam, *Proportionality and Force in International Law*, 87 AMERICAN JOURNAL OF INTERNATIONAL LAW 391 (1993).

83. PROTOCOLS ADDITIONAL COMMENTARY, *supra* note 26, para. 2209.

84. A number of understandings/declarations/reservations have been issued on this point by Parties to Protocol Additional I. For instance, the United Kingdom made the following reservation when ratifying the protocol in 1998: "In the view of the United Kingdom, the military advantage anticipated from an attack is intended to refer to the advantage anticipated from the attack

considered as a whole and not only from isolated or particular parts of the attack." ICRC website, *supra* note 76.

85. An additional problem is that the valuation process itself is complex. For instance, culture may determine the value placed on an item or the value of an item may shift over time. The issue of valuation paradigms is explored, in the context of environmental damage during armed conflict, more fully in Michael N. Schmitt, *War and the Environment: Fault Lines in the Prescriptive Landscape*, 37 ARCHIV DES VOLKERRECHTS 25 (1999).

86. PROTOCOLS ADDITIONAL COMMENTARY, *supra* note 26, para. 1978.

87. *NATO Denies Targeting Water Supplies*, BBC WORLD ONLINE NETWORK, May 24, 1999, http://news.bbc.co.uk/hi/english/world/europe/newsid_351000/351780.stm.

88. *See generally*, Protocol Additional I, *supra* note 10, art. 57.

89. The Joint Warfare Analysis Center currently is engaged in modeling foreign infrastructures and contingent outcomes.

90. *Id.*, art. 57.2(a).

91. *Id.*, art. 57.3.

92. Article 39 of Additional Protocol I prohibits the use of the enemy's military emblems, insignia or uniforms. This prohibition, which the United States disagrees with except when it occurs during the actual engagement (*see* Handbook, *supra* note 54, para 12.1.1, fn 2), does not extend to the use of codes, passwords, and the like. MICHAEL BOTHE, KARL J. PARTSCH & WALDEMAR A. SOLF, NEW RULES FOR VICTIMS OF ARMED CONFLICTS (1982). However, Article 38 prohibits the misuse of protective signals.

93. Protocol Additional I, *supra* note 10, art. 37. *See also* Rome Statute, *supra* note 58, art. 8.2(b)(vii) & (xi). Convention (IV) respecting the Laws and Customs of War on Land, Oct. 18, 1907, annexed Regulations, art. 23(b)7, 36 Stat. 2277, 205 Consolidated Treaty Series 277, *reprinted in* ROBERTS & GUELFF, *supra* note 10, at 73, prohibits treacherous killing.

94. Protocol Additional I, *supra* note 10, annex, art. 11.

95. Office of General Counsel, Department of Defense, An Assessment of Legal Issues in Information Operations (Nov. 1999). The paper is appended to this volume as the Appendix.

96. *Id.*, art. 37.1(c); US Army Judge Advocate General's School, Operational Law Handbook 5-16 (2000).

97. Protocols Additional Commentary, *supra* note 10, paras. 1492–94.

98. GC IV, *supra* note 19, art. 28; Protocol Additional I, *supra* note 10 art. 51.7. *See also* Rome Statute, *supra* note 58, art. 8.2(b)(xxiii); Hans P. Gasser, *Protection of the Civilian Population*, *in* THE HANDBOOK OF HUMANITARIAN LAW IN ARMED CONFLICT 209, 218 (Dieter Fleck ed., 1995).

99. Protocol Additional I, *supra* note 10, art. 47.2. The United States does not support Article 47.

100. *Id.*, art. 47.1. This is problematic because States Party to the International Convention against the Recruitment, Use, Financing and Training of Mercenaries, albeit limited in number and though the convention is not yet in force (it has only secured 21 of the 22 necessary ratifications as of October 2001), are obligated to amend their domestic laws to outlaw mercenarism. GA Res. 44/34 (1989), art. 5.3, ICRC website, *supra* note 76.

101. For a description of hesitancy to use CNA during Operation ALLIED FORCE, see Bradley Graham, *Military Grappling with Rules for Cyber Warfare: Questions Prevented Use on Yugoslavia*, WASHINGTON POST, Nov. 8, 1999, at A1.

102. *See* Schmitt, *Computer Network Attack*, *supra* note 7.

103. Consider the comment of Lieutenant General Michael Short, USAF, who commanded the air war during Operation ALLIED FORCE:

> I felt that on the first night, the power should have gone off, and major bridges around Belgrade should have gone into the Danube, and the water should be cut off so that the next

morning the leading citizens of Belgrade would have got up and asked, "Why are we doing this?" and asked Milosovic the same question.

Craig R. Whitney, *The Commander: Air Wars Won't Stay Risk-Free, General Says*, THE NEW YORK TIMES, June 18, 1999, at A1.

104. PROTOCOLS ADDITIONAL COMMENTARY, *supra* note 26, para. 1871, notes that "it is the duty of Parties to the conflict to have the means available to respect the rules of the Protocol. In any case, it is reprehensible for a Party possessing such means not to use them, and thus consciously prevent itself from making the required distinction."

105. A typical Information Operations cell is illustrated in Joint Pub 3-13, *supra* note 2, at figure IV-4 and accompanying text. It includes an IO officer from J-3; representatives from J-2, 4, 5, 6, 7, supporting combatant commands, and service and functional components; a judge advocate; and public affairs, counterintelligence, civil affairs, targeting, special operations, special technical operations, electronic warfare, psychological operations, military deception, and operations security experts.